Comparative study of Internet of Things infrastructure and security

Singh, Bhupjit; Kaur, Bipjeet

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Comparative study of Internet of Things Infrastructures & Security

Bhupjit Singh
DTU Diplom
Technical University of Denmark
Ballerup, Denmark
bhsi@dtu.dk

Bipjeet Kaur
DTU Diplom
Technical University of Denmark
Ballerup, Denmark
bika@dtu.dk

***Abstract*— With increasing use of IoTs in diverse fields has increased the demands of different parameters for high level of security, trust and applications. Several companies have invested millions of dollar to fulfill the needs of the market which has given rise variant infrastructures of IoTs. In this paper we have compared the different infrastructures and their parameters along with establishing the requirements of security in IoTs. The various vulnerabilities in the IoTs architecture and consideration for privacy control is also discussed. After identifying the security issues in IoTs , this paper suggests solutions from existing technologies as a starting point for establishing a standardized security paradigm in IoTs**

Keywords—LoRaWAN; SigFox; Symphony; IoT architecture; requirements for security paradigm in IoTs; security issues in IoTs;IoTs Security

I. INTRODUCTION

The term Internet of Things (IoT) has gained enormous popularity with the explosion of wireless sensor networks, smart meters, home automation devices, and wearable electronics. The IoT spans long-range outdoor networks such as the smart grid and municipal lighting, as well as shorter-range indoor networks that enable the connected home and residential security systems. Each year will see exponential growth in devices connected to the Internet. Gartner predicts there will be 25 billion connected “things” by 2020. [1] It is not matter of things but actually connectivity and services.

Numerous companies have introduced innovative solutions for the IoT market that provide security, status, and other convenient services. A connected system architecture comprises a number of wireless nodes ranging from simple remote control devices to complex wireless networks featuring a gateway to connect to the Internet. One of the major issues for machine to machine, M2M communications used for applications like the Internet of Things, IoT is to enable communications over long ranges using very low power levels [2].

This paper is divided into six sections; Introduction, Infrastructure Of IoTs, Comparative Study Of IoT Infrastructure, General Architecture of IoTs Network, Security Issues in IoTs Networks, Conclusion and Future Work

II. INFRASTRUCTURES OF IOT

A. LoRaWAN

One scheme for addressing long range communication dedicated to Internet of things is known as LoRa. It gains its name from the fact that it is able to provide 'LongRange' communications using very low power levels. It uses low-power, long-range wireless connectivity in the widely used sub-GHz band.

It is a LPWAN (Low-Power Wide-Area network)), currently deployed in Western Europe, San Francisco, and with ongoing tests in South America & Asia. These are best suited for connecting devices that need small amount data and long battery life.

Actually LoRaWAN is based on server-side implementation of a multiple access protocol. It is specially designed to minimize collisions with a large number of endpoints. It requires a server application to run the MAC functions over a network connection. Its architecture is typically laid out in a star-of-stars topology in which gateways are a transparent bridge relaying messages between end-devices and a central network server in the backend.

It is designed primarily for uplink-only applications with many endpoints, or applications where only a few downlink messages are required (limited either by application or by number of endpoints). In this type of architecture, the gateway within the same network require synchronization. Communication between end-devices and gateways is spread out on different frequency channels and data rates. The selection of the data rate is a trade-off between communication range and message duration. Different data rates do not interfere with each other instead create a set of “virtual” channels increasing the capacity of the gateway.

The LoRaWAN network server is manages the data rate and RF output for each end-device individually by means of an adaptive data rate (ADR) scheme that is typically updated once every 24 hours. Multiple layers of security/encryption (EUI64 on network level and application level and EUI128

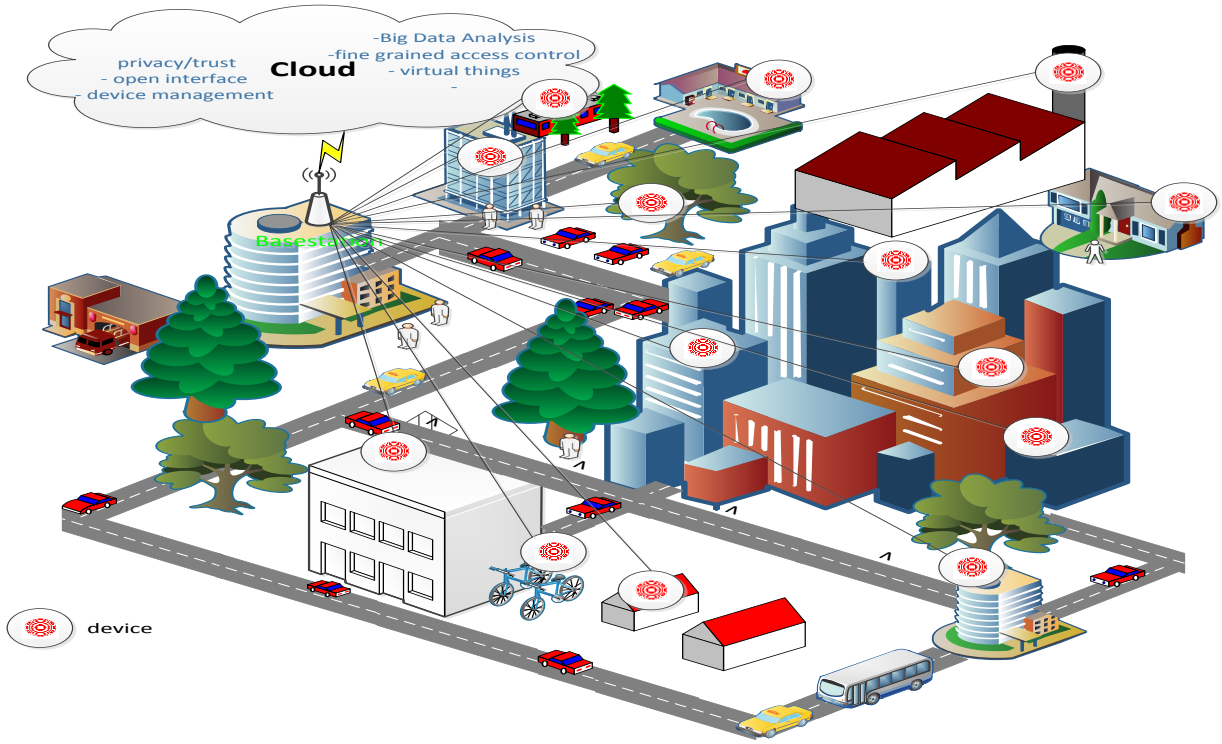

Figure:1 IoT Network in Smart City Application

device specific key). AES CCM (128-bit) for encryption and authentication is available in this infrastructure. It works within the confines of the ETSI 1% and 10% duty cycle on transmission time in the 868 bands. Draft revision of class B for downlink nodes that can poll for a beacon every 1s to 128s (2^n) where n is 0 to 7. It has also got antenna diversity. It is due to that all gateways' listen to the same uplink channels. LoRaWAN has Adaptive Data Rate which is driven by the server, if a node's link suddenly fades, the server has no way of telling it to change spreading factors to compensate. ADR for LoRaWAN issued to optimize the capacity of the channel.

B. SigFox

SIGFOX is an operated telecommunication network, dedicated to the Internet of Things. It is an operated network, meaning you do not have to handle any installation or maintenance operations.

SIGFOX is seamless and out-of-the box, allowing you to forget about communication and keep focused on the core of your project. SIGFOX is operational in 24 countries covering about 1.4 million Km^2 and 358 million people. This is world largest IoT network.

SIGFOX allows a bidirectional communication, both from & to the device. The communication is always initiated by the device. The SIGFOX network is designed for small messages sent every now and then. It is not appropriate for high-bandwidth usages (multimedia, permanent broadcast). Its focus on energy efficiency allows you to build connected devices able to last years on a standard battery.

SigFox sets up antennas on towers (like a cell phone company), and receives data transmissions from devices like parking sensors or water meters. These transmissions use frequencies that are unlicensed, which in the US is the 915 MHz ISM band; the same frequency a cordless phone uses. (Europe has a narrower band around 868 MHz, and most of the world has some version of this band either like the US or Europe, all with different rules that govern their use.) SigFox wireless systems send very small amounts of data which is 12 bytes and at very slow rate of 300 baud using standard radio transmission methods namely phase-shift keying – DBPSK – uplink and frequency-shift keying – GFSK –downlink. The long range is therefore accomplished by very long and very slows messages. This technology is a good fit for any application that needs to send small, not very frequent bursts of data. Examples such as basic alarm systems, location monitoring, and simple metering are one-way systems that might make use of such network infrastructure. In these networks, the signal is typically sent a few times to "ensure" the message goes through. While this works, there are some limitations, such as shorter battery life for battery-powered applications, and an inability to guarantee a message is actually received by the tower.

Another way to design a network is bi-directionally (like your cell phone). SigFox has not deployed any bi-directional networks, though they have said to be working on the technology. If they are successful in deploying a two-way

network, this will enable a wider variety of applications on their networks, though it will not have a symmetrical link because of the underlying technology they have chosen.
SigFox has faced challenges in US due the law that limits the use of the unlicensed radio spectrum with the maximum transmission time on the air to be 0.4 seconds. But SigFox transmissions are 3 seconds or so, this makes too difficult to enter the market and now it requires a new architecture design. The frequency band in the US is also subject to much higher levels of interference than the band SigFox uses in Europe. This issue has brought problem in SigFox business for example: the pet tracking company, Whistle, announced a partnership to sell a solution on the SigFox wireless network in May 2014, but has been unable to ship product.

C. Symphony

It is developed by Link-labs to overcome the pitfalls of the LoPoWAN. It guarantees message receipt. There is very high loss of packets in case of SigFox and LoPoWAN. Symphony link acknowledges every message both in uplink and downlink. It uses light TCP like architecture.
Symphony Link allows updates the host firmware on the device after it has been fielded. This is huge advantage early in the IoT evolution, as it allows customers to get to market more quickly, and with less risk. This lowers the network management struggles in case of networks with hundreds of device in large networks.

Symphony Link uses the Frequency Hopping Listen Before Talk plus adaptive frequency agility band, thus removes the duty cycle limit. In the 900 MHz Band, there is no duty cycle limit. The duty cycle of 1% prevents LoRaWAN from being used in systems that need the ability to send lots of data at a time. Since Symphony Link is a synchronous protocol, repeaters allow users to expand the range of the network dramatically without impacting latency.
In Symphony Link, the host device configuration is the same for all devices of the same type, and key exchange is handled via PKI based Diffie Hellman AES architecture. Symphony Link infrastructure, before every transmission, an end device calculates the reverse link to the gateway, and adjusts its transmit power and spreading factor or modulation rate to match. This way node throughout the network has a balanced link budget. Close nodes are transmitting quietly and quickly, and far nodes are transmitting loudly and slowly. ADR in Symphony Link is about optimizing performance and reliability. Symphony Link uses a dynamic channel mask that is controlled by the gateway, it ensures as few collisions as possible. By using asynchronous features like slotting, and uplink/downlink coordination, a Symphony Link network has over 4 times the capacity of LoRaWAN. And when you couple that with quality of service, Symphony Link is a much more robust choice for users that need it.

III. COMARATIVE STUDY OF IOT INFRASTRUCTURES

No single architecture and service provider can cover all the application and services needed for the diversity applications in the world of internet of things. Each service provider aims at high availability and intensive level of services but security in Internet of things restricts its way. The Figure:1 shows the comparison between different IoT infrastructure. The internets of things' networks are highly vulnerable to security risks.

	Range	Data rates	Power consumption	Duty Cycle	Modulation
LoRaWAN	10km Bidirectional	5000 bit/s	5-10 years	1%	chirped spread spectrum (CSS)
SigFox	Bidirectional	12 bytes/s	Less than 5 years	1%	BPSK
Symphony	Greater than 10 km Bidirectional	Adaptive Data Rate	7-10 years	No limit	Frequency hopping plus adaptive frequency agility band

Table:1 Compartive table at different IoT infrastructures

IV. GENERAL ARCHITECTURE OF IOT NETWORKS

Figure 1 shows the smart city infrastructure in which a single base station can cover several devices and the cloud solution will provide privacy, trust–open interface, device management,
The IoT Architecture can be stacked into 4 layers in which the most basic level layer is the perceptual layer (also known as recognition layer), which collects all kinds of information through physical equipment and identifies the physical world, the information includes object properties, environmental condition etc; and physical equipment include RFID reader, all kinds of sensors, GPS and other equipment. The key component in this layer is sensors for capturing and representing the physical world in the digital world. The second level is network layer. Network layer is responsible for the reliable transmission of information from perceptual layer, initial processing of information, classification and polymerization. In this layer the information transmission is relied on several basic networks, which are the internet, mobile communication network, satellite nets, wireless network, network infrastructure and communication protocols are also essential to the information exchange between devices.
The third level is Data Fusion layer. This layer will set up a reliable support platform for the application layer, on this support platform all kind of intelligent computing powers will be organized through network grid and cloud computing. It plays the role of combining application layer upward and network layer downward.
The application layer is the topmost and terminal level. Application layer provides the personalized services according

to the needs of the users. Users can access to the internet of thing through the application layer interface using of television, personal computer or mobile equipment and so on. Network security and management play an important role in above each level. Then we will analysis the security features.

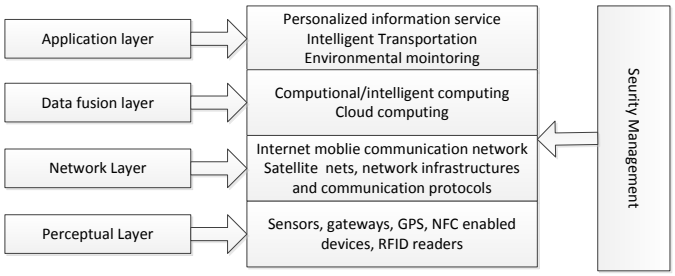

Figure 2: Internet of things layered architecture

V. Security Issues in IoTs

The issue of security is one of the most important issues considered as IoTs devices should be able to communicate in heterogeneous system to provide on the clock service in a long term deployment without having to perform regular checks. This setup leads to various intermittent and locale specific failures and could also lead to more permanent failures. Some of these failures in IoTs are covered by the obvious redundancy that is needed in such kind of deployments but due to the demand for IoTs to perform consistently and have the ability to recover from security attacks to normal operations. Thus, the security solution should cover the possibility of security updates, easy connection, attack detection capabilities with a standardization in IoT architecture among all layers to operate in different modes to provide networking with the bare minimum services in order to convey and recover from various security attacks. These modes would be able to provide attack detection, diagnose, apply repairs and countermeasures, there is also the need to keep in mind the computational limitations of IoTs while building such a security solution [9]. To recover and repair, it is sometimes needed to go offline, reprogram, go into recovery modes. Thus, in order to switch between recovery mode and other modes which might be without networking, ad hoc connections with easy connection, authentication and small overheads for configuration of network with light weight security techniques will be needed. The above mentioned factors are a good starting point for the security paradigm in IoTs.

The data protection and privacy is one of the key aspects with respect to IoT as access control of data should ultimately be the decision of the user.

Access control in IoTs has to consider aspects such that limiting or granting access is on the discretion of user. It should possible to give and remove access to various systems involved, on the fly with some kind of leasing. The type of access to data should also be determent to context of data usage, that is the data available from IoTs should be categorized into various data sets with heuristic trust- so that data is only to be used in specific context. Certain assurances and certification could also be provided that data would not be used out of context of pre agreed terms (some legislations and other policies would be needed to be passed in order to fully
realize this aspect [9])[10].

Influenced by existing solution, data distortion and data encryption is the driving force along with key management and authentication as IoTs integration is within heterogeneous, multi-layer networks. [10]

Identify security issues in the specific layers: [11,14]

1. Security challenges faced in perceptual layer are node authentication, confidentiality of information. Attacks like distributed denial of service and poor physical security with respect to installation of IoTs “things” cause separate set of problems.
2. In network layer security attacks like man in the middle attack and counterfeit attack are experienced along with data congestion and other problems relating to network layer are consistent in this layer. As perceptual layer and network layer are very closely related, problems like exploiting devices through unsecure network services are common in this layer.
3. In data fusion layer, malicious information, attacks from internet due to lack of transport encryption, insufficient authentication are common along with other insecure cloud interface.
4. In Application layer privacy protection due to data sharing plays an important role with respect to access control along with all the implications of data privacy. The data fusion layer works closely with application layer thus the issues from data fusion layer related to data integrity and corruptness creeps in this layer.

Proposed security solution

To deal with various security issues identified in the above section, a need for a framework specific for IoT security and privacy which has layer specific attack detection and repair capabilities (discussed in detail in next paragraph) along with privacy constraints. It should be able to determine and define the context of data in real time and dynamic propose privacy policies on the fly. It should also be able to facilitate secure inter domain data interaction and data fetching or querying in line with the various aspect of data access control discussed above.

In perceptual layer, equipment backup or limiting access to the site could be one immediate solution to counter poor physical installation of nodes. Illegal node access could be avoided by node authentication based on various attributes of the hardware by means of a digital certificate within the confines of the extranet established by VPNs to provide data integrity and confidentiality between nodes to gateway.

In network layer, there exist a set of communication security solution but it is difficult to be applied in IoT systems, as it should contain identity authentication along with confidentiality and integrity mechanism, thus public- key cryptography to sign resources to guarantee origin authenticity and integrity of delivered information. IPSec in network layer can provide integrity, authenticity and confidentiality. But to counter DDos

attacks due to less processing power can be quite severe, limiting access to the nodes to only through VPN could provide some control but on the other hand gateways needs enhanced processing and inter domain communication capabilities.
In the data fusion layer, there are various kind of solutions like strong encryption algorithms, data validation algorithms along with other data verification logics can be applied with existing two factor, heavy weight encryption. The cloud based web interface should not be susceptible to XSS, SQLi, CSRF with bogus attempt detection capabilities.
In the application layer, key agreement across heterogeneous networks is a key aspect which can be covered by the existing solutions, but the privacy aspect of privacy protection is discussed in the conclusion. TLS/ SSL protocols while transiting networks, with message payload encryption with key handshaking and data verification are needed in this layer.

VI. Conclusion and Future Work

To conclude the security issues in IoT, communication security and data privacy are two different aspects of security which should be addressed in their own right. The data protection should be such that, it should provide a balance between providing access to data. Its aim is to achieve full exploitation of data to reap benefits of IoTs without users worrying about repercussion and implications for providing access to their private data. This could be achieved via Anonymity and Pseudonymity[15,16] along with legislations and heuristic trust solutions which could provide access to the data with respect to the context of data usage.
The aspect of communication security has couple of key points to be considered, firstly, security solutions should be light weight due to the limitation of computational power of IoTs especially in perceptual and network layer. Secondly, it should have the ability to detect and repair the IoT nodes themselves. This can be achieved by establishing standardized secure communication framework which would include troubleshooting, recovery modes to perform attack detection and self-repair. This framework expands and adapts its services, functionality and security patching to cover layer specific failures and security risk but keeps the bare bone structure running in a virtual environment.
Looking into proposed solution we intend to work into extension of design and implementation of proposed framework in several areas of applications of IoT Networks

Acknowledgment

This project is carried out in close collaboration with Prof. Dr. Joseph Kueng, Institute for Application Oriented Knowledge Processing, JKU, Linz. This research was funded by the FP7 - EU FRAMEWORK PROGRAMME under grant agreement No. 604659 (project CLAFIS).

References

[1] http://www.gartner.com/newsroom/id/2905717
[2] J. Allmendinger, G., Lombreglia, R.: Four Stages for the Age of the Smart Services (2012) http://courses.ischool.berkeley.edu/i2901/f08/readings/StrategiesSmartServices.pdf
[3] IBM Market Insights, Cloud Computing Strategy Research, July 2009
[4] Low Power Wide Area Network Technology : Symphony Link vs. LoRaWAN A Guide for Engineers and Decision Makers. White paper links lab 2016
[5] A Comprehensive Look at Low Power, Wide Area Networks For 'Internet of Things' Engineers and Decision Makers
[6] C. tian, X. Chen et.al : Analysis and Design of Security in Internet of Things, 8th International Conference on BioMedical Engineering and Informatics, 2015.
[7] Advances in Cyber-Physical Systems Research :Jiafu Wan, Hehua Yan, Hui Suo and Fang Li
[8] The research of several key question of Internet of Things: Zhihua Hu
[9] Internet of Things – New security and privacy challenges: Rolf H. Weber - University of Zurich, Zurich, Switzerland, and University of Hong Kong, Hong Kong
[10] H Suo, J. Wan Security in the internet of things: Review, 2012 International Conference on computer Science and Electronics Engineering
[11] John A. Stankovic, Life Fellow, IEEE "Research Directions for the Internet of Things"
[12] A comprehensive look at Low Power, Wide Area Networks For 'Internet of Things' Engineers and Decision Makers
[13] G.Gang, LU Zeyong: Internet of Things Security Analysis
[14] https://www.owasp.org/index.php/Top_IoT_Vulnerabilities
[15] Security and Privacy Grand Challenges for the Internet of Things : Glenn A Fink, Dimittri V. Zarzhitsky, Thomas E Carroll and Ethan D Farquhar
[16] The Information Security for the Application of IoT Technology : Jia Jiang and Donghai Yang
[17] LoRa vs LTE-M vs Sigfox - http://www.nickhunn.com/lora-vs-lte-m-vs-sigfox/
[18] http://pages.silabs.com/rs/silabs/images/Wireless-Connectivity-for-IoT.pdf?mkt_tok=3RkMMJWWfF9wsRoguKjNZKXonjHpfsX86+4rWKK3lMI/0ER3fOvrPUfGjI4DSsJkI+SLDwEYGJlv6SgFTLPBMbNsz7gOXBg
[19] http://link.springer.com/chapter/10.1007/978-3-662-43871-8_243?no-access=true
[20] https://www.link-labs.com/what-is-sigfox/
[21] http://web.gdmec.cn/zlgcxm/2013/jxgg/xxljq/support/%E5%88%98%E5%BB%BA%E5%9C%BB/%E8%AE%BA%E6%96%87/Security%20in%20the%20internet%20of%20things%20A%20review.pdf
[22] http://www.radio-electronics.com/info/wireless/lora/basics-tutorial.php